UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/609,260	06/26/2003	Ramarathnam Venkatesan	MS1-1043US	8086

22801 7590 05/17/2007

LEE & HAYES PLLC
421 W RIVERSIDE AVENUE SUITE 500
SPOKANE, WA 99201

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

NOTIFICATION DATE	DELIVERY MODE
05/17/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

Office Action Summary	Application No.	Applicant(s)	
	10/609,260	VENKATESAN ET AL.	
	Examiner	Art Unit	
	Michael J. Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 March 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-73* is/are pending in the application.

4a) Of the above claim(s) *48-73* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 June 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *6/26/03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The IDS of 6/26/2003 was received and considered.

2. Claims 1-73 are pending.

Election/Restrictions

3. Claims 48-73 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected species, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 3/12/2007.

Claim Objections

4. Claims 5-7, 17-19 & 36-47 are objected to because of the following informalities:

   a. Regarding claim 5, line 2, "using with" should be replaced with "with";

   b. Regarding claim 17, line 2, "using with" should be replaced with "with";

   c. Regarding claim 36, line 4, "using parameter data configure" should be replaced with "using parameter data to configure".

   d. Regarding claim 42, line 5, "using parameter data configure" should be replaced with "using parameter data to configure".

5. Appropriate correction is required.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1-7 & 36-41 are rejected under 35 U.S.C. 102(b) as being anticipated by "*Short Signatures from the Weil Pairing*" by Boneh et al. (**Boneh**), published December 9-13, 2001.

Regarding claim 1, Boneh discloses identifying data to be signed (message M, p. 516, §2.2, Signing & p. 524, §3.5, Signing), establishing parameter data (base group G, generator g, §2.2, ¶1) for use with signature generating logic (GDH signature scheme, p. 516) that encrypts data (h^x, p. 516, Signing) based on a Jacobian of a curve (p. 517, §3, ¶1) & p. 525, ¶3) having a genus exceeding one (genus 2, p. 525, ¶3), said parameter data causing said signature generating logic to select at least one Gap Diffie-Hellman (GDH) group of elements (p. 516, last paragraph & p. 517, §3, ¶1) relating to said curve, determining private key data (x, p. 516, Key generation) and corresponding public key data (v, p. 516, Key generation) using said signature generating logic (GDH signature scheme, §2.2), and signing said identified data (M) with said private key data (h^x, p. 516, Signing) using said signature generating logic (GDH signature scheme) to create a corresponding digital signature (σ, p. 516, Signing).

Regarding claim 2, Boneh discloses wherein said identified data includes a message $m \in \{0,1\}*$ (p. 516, §2.2, Signing).

Regarding claim 3, Boneh discloses wherein said parameter data establishes a base group G and a generator g as system parameters (§2.2, ¶1) for said signature generating logic (GDH signature scheme, §2.2, ¶1).

Regarding claim 4, Boneh discloses wherein determining said private key data and said public key data includes picking $x \xleftarrow{R} Z^*_p$ (p. 516, Key generation) and computing $v \leftarrow g^x$

(p. 516, Key generation), wherein said public key data includes v and said private key data includes x (p. 516, Key generation).

Regarding claim 5, Boneh discloses wherein signing said identified data (M) using said private key data (x) using said signature generating logic (GDH signature scheme) further includes determining $h \leftarrow h(m)$, and $\sigma \leftarrow h^x$, using at least one hash function (p. 516, Signing), said private key data x and said message m (p. 516, Signing), wherein said digital signature includes σ (p. 516, Signing).

Regarding claim 6, Boneh discloses wherein said hash function includes a full-domain hash function (p. 516, §2.2, ¶2).

Regarding claim 7, Boneh discloses wherein said hash function (p. 520, §3.3, ¶2) includes a hash function h': $\{0,1\}^* \rightarrow G \cup \{\perp\}$ that outputs an element of G or $\perp$ indicating a failure (p. 521, MapToGroup, step 3b; outputs P_M, an element of G or increments and repeats, or eventually reports a failure).

Regarding claim 36, Boneh discloses receiving message data (M) and a corresponding digital signature (σ) and public key data (v=public key, G=group system parameter, g=generator, i.e. given V, M, σ, G, h and g, p. 516, §2.2, Verification), using parameter data (G and g) to configure signature verifying logic (GDH signature scheme, p. 516, Verification) that performs cryptography operations (verification) based on a Jacobian of a curve (p. 517, §3, ¶1 & p. 525, ¶3), said Jacobian having a genus greater than one (genus 2, p. 525, ¶3), said parameter data (G and g) causing said signature verifying logic to select at least one Gap Diffie-Hellman (GDH) group of elements relating to said curve (system parameter G and generator g; note that the signature σ is an element of G), and with said signature verifying logic (GDH signature

scheme), determining if said digital signature is valid (p. 516, §2.2, Verification) using said public key (v) and said message data (M) (p. 516, §2.2, Verification.

Regarding claim 37, Boneh discloses wherein said message data includes a message $m \in \{0,1\}^*$ (p. 516, §2.2, Signing).

Regarding claim 38, Boneh discloses wherein said parameter data establishes a base group G and a generator g as system parameters (§2.2, ¶1) for said signature generating logic (GDH signature scheme, §2.2, ¶1).

Regarding claim 39, Boneh discloses wherein said public key data (v) includes public key data v (p. 516, Key generation), said digital signature includes signature σ (p. 516, Key generation) and determining if said digital signature is valid further includes determining $h \leftarrow h(m)$ using at least one hash function (p. 516, Verification) and verifying that (g, v, h, σ) is a valid Gap Diffie-Hellman tuple (p. 516, Verification).

Regarding claim 40, Boneh discloses wherein said hash function includes a full-domain hash function (p. 516, §2.2, ¶2).

Regarding claim 41, Boneh discloses wherein said hash function (p. 520, §3.3, ¶2) includes a hash function h': $\{0,1\}^* \rightarrow G \cup \{\perp\}$ that outputs an element of G or $\perp$ indicating a failure (p. 521, MapToGroup, step 3b; outputs P_M, an element of G or increments and repeats, or eventually reports a failure).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 13-19, 24-30 & 42-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Boneh** in view of what is well known in the art.

Regarding claim 13, the claim is substantially equivalent to claim 1 with the exception that it recites a computer-readable medium with instructions for causing at least one processing unit to perform the method. However, it is well known in the art of computers and cryptography to automate algorithms using computer instructions that cause at least one processing unit to carry out the algorithm (method). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Boneh to embody the method disclosed in executable instructions embodied on a computer-readable medium for causing at least one processing unit to execute the instructions. One of ordinary skill in the art would have been motivated to perform such a modification to automate the algorithm, as is well known in the art.

Regarding claim 14, Boneh discloses wherein said identified data includes a message $m \in \{0,1\}^*$ (p. 516, §2.2, Signing).

Regarding claim 15, Boneh discloses wherein said parameter data establishes a base group G and a generator g as system parameters (§2.2, ¶1) for said signature generating logic (GDH signature scheme, §2.2, ¶1).

Regarding claim 16, Boneh discloses wherein determining said private key data and said public key data includes picking $x \xleftarrow{R} Z^*_p$ (p. 516, Key generation) and computing $v \leftarrow g^x$ (p. 516, Key generation), wherein said public key data includes v and said private key data includes x (p. 516, Key generation).

Regarding claim 17, Boneh discloses wherein signing said identified data (M) using said private key data (x) using said signature generating logic (GDH signature scheme) further includes determining $h \leftarrow h(m)$, and $\sigma \leftarrow h^x$, using at least one hash function (p. 516, Signing), said private key data x and said message m (p. 516, Signing), wherein said digital signature includes σ (p. 516, Signing).

Regarding claim 18, Boneh discloses wherein said hash function includes a full-domain hash function (p. 516, §2.2, ¶2).

Regarding claim 19, Boneh discloses wherein said hash function (p. 520, §3.3, ¶2) includes a hash function h': $\{0,1\}^* \rightarrow G \cup \{\perp\}$ that outputs an element of G or $\perp$ indicating a failure (p. 521, MapToGroup, step 3b; outputs P_M, an element of G or increments and repeats, or eventually reports a failure).

Regarding claim 24, the claim is substantially equivalent to claim 1 with the exception that it recites an apparatus that performs the method and comprises memory configured to store identifying data that is to be signed. However, it is well known in the art of computers and cryptography to automate algorithms using computers to carry out the algorithm (method) and that computers use memory to store data to be operated upon. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Boneh to embody the method disclosed therein in an apparatus to generate the keys and sign the

data, comprising memory configured to store identifying data that is to be signed. One of ordinary skill in the art would have been motivated to perform such a modification to automate the algorithm, as is well known in the art.

Regarding claim 25, Boneh discloses wherein said identified data includes a message $m \in \{0,1\}^*$ (p. 516, §2.2, Signing).

Regarding claim 26, Boneh discloses wherein said parameter data establishes a base group G and a generator g as system parameters (§2.2, ¶1) for said signature generating logic (GDH signature scheme, §2.2, ¶1).

Regarding claim 27, Boneh discloses wherein determining said private key data and said public key data includes picking $x \xleftarrow{R} Z^*_p$ (p. 516, Key generation) and computing $v \leftarrow g^x$ (p. 516, Key generation), wherein said public key data includes v and said private key data includes x (p. 516, Key generation).

Regarding claim 28, Boneh discloses wherein signing said identified data (M) using said private key data (x) using said signature generating logic (GDH signature scheme) further includes determining $h \leftarrow h(m)$, and $\sigma \leftarrow h^x$, using at least one hash function (p. 516, Signing), said private key data x and said message m (p. 516, Signing), wherein said digital signature includes σ (p. 516, Signing).

Regarding claim 29, Boneh discloses wherein said hash function includes a full-domain hash function (p. 516, §2.2, ¶2).

Regarding claim 30, Boneh discloses wherein said hash function (p. 520, §3.3, ¶2) includes a hash function h': $\{0,1\}^* \rightarrow G \cup \{\perp\}$ that outputs an element of G or $\perp$ indicating a

failure (p. 521, MapToGroup, step 3b; outputs P_M, an element of G or increments and repeats, or eventually reports a failure).

Regarding claim 42, the claim is substantially equivalent to claim 36 with the exception that it recites a computer-readable medium with instructions for causing at least one processing unit to perform the method. However, it is well known in the art of computers and cryptography to automate algorithms using computer instructions that cause at least one processing unit to carry out the algorithm (method). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Boneh to embody the method disclosed in executable instructions embodied on a computer-readable medium for causing at least one processing unit to execute the instructions. One of ordinary skill in the art would have been motivated to perform such a modification to automate the algorithm, as is well known in the art.

Regarding claim 43, Boneh discloses wherein said message data includes a message $m \in \{0,1\}^*$ (p. 516, §2.2, Signing).

Regarding claim 44, Boneh discloses wherein said parameter data establishes a base group G and a generator g as system parameters (§2.2, ¶1) for said signature generating logic (GDH signature scheme, §2.2, ¶1).

Regarding claim 45, Boneh discloses wherein said public key data (v) includes public key data v (p. 516, Key generation), said digital signature includes signature σ (p. 516, Key generation) and determining if said digital signature is valid further includes determining $h \leftarrow h(m)$ using at least one hash function (p. 516, Verification) and verifying that (g, v, h, σ) is a valid Gap Diffie-Hellman tuple (p. 516, Verification).

Regarding claim 46, Boneh discloses wherein said hash function includes a full-domain hash function (p. 516, §2.2, ¶2).

Regarding claim 47, Boneh discloses wherein said hash function (p. 520, §3.3, ¶2) includes a hash function h': $\{0,1\}^* \rightarrow G \cup \{\perp\}$ that outputs an element of G or $\perp$ indicating a failure (p. 521, MapToGroup, step 3b; outputs P_M, an element of G or increments and repeats, or eventually reports a failure).

10. Claims 8-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Boneh**.

Regarding claim 8, Boneh lacks outputting the digital signature. However, Boneh teaches that digital signatures are used in environments where a human is asked to manually key in the signature provided on a CD label or postage stamp (§1, ¶1). In such a situation, one of ordinary skill in the art understands that the signature on the label must have been created and then outputted to the CD label or postage stamp. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Boneh's implementation-generic signature scheme to output the created signature to a CD label or postage stamp. One of ordinary skill in the art would have been motivated to perform such a modification to use the created signature as a postage stamp, as taught by Boneh (§1, ¶1).

Regarding claim 9, Boneh discloses determining if said digital signature is valid using signature verifying logic (GDH signature scheme, Verification, p. 516).

Regarding claim 10, Boneh discloses wherein said signature verification logic (GDH signature scheme) is configured using said parameter data (g and G) and said parameter data establishes base group G and generator g as system parameters for said signature verifying logic

(verification logic is given system parameters and specifically uses g, v, h, σ, p. 516, §2.2, verification).

Regarding claim 11, Boneh discloses wherein said public key data (v) includes public key data v (p. 516, Key generation), said identified data includes a message *m*, said digital signature includes signature σ (p. 516, Key generation) and determining if said digital signature is valid further includes determining $h \leftarrow h(m)$ using at least one hash function (p. 516, Verification) and verifying that (g, v, h, σ) is a valid Gap Diffie-Hellman tuple (p. 516, Verification).

Regarding claim 12, Boneh lacks wherein the signature is included in a product ID. However, Boneh teaches that digital signatures are used in environments where a human is asked to manually key in the signature provided on a CD label (§1, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Boneh's implementation-generic signature scheme to include the created signature in a product ID (CD label). One of ordinary skill in the art would have been motivated to perform such a modification to use the created signature for product registration, as taught by Boneh (§1, ¶1).

11. Claims 20-23 & 31-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Boneh**, as modified above with respect to claims 13 & 24.

Regarding claim 20, Boneh lacks outputting the digital signature. However, Boneh teaches that digital signatures are used in environments where a human is asked to manually key in the signature provided on a CD label or postage stamp (§1, ¶1). In such a situation, one of ordinary skill in the art understands that the signature on the label must have been created and then outputted to the CD label or postage stamp. Therefore, it would have been obvious to one

having ordinary skill in the art at the time the invention was made to modify Boneh's implementation-generic signature scheme to output the created signature to a CD label or postage stamp. One of ordinary skill in the art would have been motivated to perform such a modification to use the created signature as a postage stamp, as taught by Boneh (§1, ¶1).

Regarding claim 21, Boneh discloses determining if said digital signature is valid using signature verifying logic (GDH signature scheme, Verification, p. 516).

Regarding claim 22, Boneh discloses wherein said signature verification logic (GDH signature scheme) is configured using said parameter data (g and G) and said parameter data establishes base group G and generator g as system parameters for said signature verifying logic (verification logic is given system parameters and specifically uses g, v, h, σ, p. 516, §2.2, verification).

Regarding claim 23, Boneh discloses wherein said public key data (v) includes public key data v (p. 516, Key generation), said identified data includes a message *m*, said digital signature includes signature σ (p. 516, Key generation) and determining if said digital signature is valid further includes determining $h \leftarrow h(m)$ using at least one hash function (p. 516, Verification) and verifying that (g, v, h, σ) is a valid Gap Diffie-Hellman tuple (p. 516, Verification).

Regarding claim 31, Boneh lacks outputting the digital signature. However, Boneh teaches that digital signatures are used in environments where a human is asked to manually key in the signature provided on a CD label or postage stamp (§1, ¶1). In such a situation, one of ordinary skill in the art understands that the signature on the label must have been created and then outputted to the CD label or postage stamp. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Boneh's

implementation-generic signature scheme to output the created signature to a CD label or postage stamp. One of ordinary skill in the art would have been motivated to perform such a modification to use the created signature as a postage stamp, as taught by Boneh (§1, ¶1).

Regarding claim 32, Boneh discloses determining if said digital signature is valid using signature verifying logic (GDH signature scheme, Verification, p. 516).

Regarding claim 33, Boneh discloses wherein said signature verification logic (GDH signature scheme) is configured using said parameter data (g and G) and said parameter data establishes base group G and generator g as system parameters for said signature verifying logic (verification logic is given system parameters and specifically uses g, v, h, σ, p. 516, §2.2, verification).

Regarding claim 34, Boneh discloses wherein said public key data (v) includes public key data v (p. 516, Key generation), said identified data includes a message *m*, said digital signature includes signature σ (p. 516, Key generation) and determining if said digital signature is valid further includes determining $h \leftarrow h(m)$ using at least one hash function (p. 516, Verification) and verifying that (g, v, h, σ) is a valid Gap Diffie-Hellman tuple (p. 516, Verification).

Regarding claim 35, Boneh lacks wherein the signature is included in a product ID. However, Boneh teaches that digital signatures are used in environments where a human is asked to manually key in the signature provided on a CD label (§1, ¶1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Boneh's implementation-generic signature scheme to include the created signature in a product ID (CD label). One of ordinary skill in the art would have been motivated to perform such a modification to use the created signature for product registration, as taught by Boneh (§1, ¶1).

Conclusion

12. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

e. U.S. Patent Application Publication 2004/0086113 and U.S. Patent 7,020,776 to Lauter et al. are cited for teaching using short signatures to create product IDs.

f. U.S. Patent Application Publication 2003/0059043 to Okeya is cited for teaching using hyperelliptic curves (specifically the Jacobian of those curves) to perform cryptographic signature operations on data.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJS

April 30, 2007

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER